



UNITED STATES DISTRICT COURT

United States of America,

v.

XUE WANG,

Defendant.

for the

Central District of California

FILED

Mar 22, 2023

 CENTRAL DISTRICT OF CALIFORNIA
 SOUTHERN DIVISION AT SANTA ANA
 BY *Nancy Boehme*
 Deputy Clerk, U.S. District Court

Case No. 8:23-mj-00173

**CRIMINAL COMPLAINT BY TELEPHONE
OR OTHER RELIABLE ELECTRONIC MEANS**

I, the complainant in this case, state that the following is true to the best of my knowledge and belief.

On or about the date(s) of March 17, 2023 in the county of Orange in the Central District of California, the defendant violated:

Code Section

18 U.S.C. § 1543

Offense Description

False Use of a Passport

This criminal complaint is based on these facts:

Please see attached affidavit.

Continued on the attached sheet.

*/s/**Complainant's signature*Daniel Ha, DHS HSI Special Agent*Printed name and title*

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by telephone.

Date: March 22, 2023**DOUGLAS F. McCORMICK***Judge's signature*City and state: Santa Ana, CaliforniaHon. Douglas F. McCormick, U.S. Magistrate Judge*Printed name and title*

AFFIDAVIT

I, Daniel Ha, being duly sworn, declare and state as follows:

I. INTRODUCTION

1. I am a Special Agent ("SA") with Homeland Security Investigations ("HSI"), and have been so employed since September 2020. I am currently assigned to the HSI Los Angeles Field Office, Orange County Assistant Special Agent in Charge Office. Prior to my employment with HSI, I was an SA with the Internal Revenue Service Criminal Investigation ("IRS-CI") for approximately 11 years. During the course of my employment with HSI and IRS-CI, I have received training including, but not limited to, various types of financial investigations, immigration fraud, and schemes to conceal and launder the proceeds of such crimes, including training at the HSI Special Agent Training Program and IRS-CI Special Agent Investigative Training Program, both at the Federal Law Enforcement Training Center in Glynco, Georgia. I have training and experience in conducting criminal investigations involving bank and wire fraud, money laundering, identity theft, and related financial crimes related to the Bank Secrecy Act. These investigations include, but are not limited to bank fraud investigations using fraudulent documents. I have also participated in the execution of search and arrest warrants involving violations of these crimes.

II. PURPOSE OF AFFIDAVIT

2. This affidavit is made in support of criminal complaints against, and arrest warrants for, Kunhua JIA ("JIA")

and XUE WANG ("WANG"), for violations of 18 U.S.C. § 1543 (False Use of a Passport).

3. This affidavit is also made in support of the following:

a. An application for a warrant to search the residence located at 86 Island Coral, Irvine, CA 92620 (the "JIA RESIDENCE"), as described more fully in Attachment A-1;

b. An application for a warrant to search a silver 2023 Porsche bearing temporary California license plate BX57G07 or California license plate 9EPD074, vehicle identification number WP0AB2A72PL130098 (the "WANG VEHICLE"), as described more fully in Attachment A-2; and

c. An application for a warrant to search the persons of KUNHUA JIA and XUE WANG, as described more fully in Attachments A-3 and A-4.

4. The requested search warrant seeks authorization to seize evidence, fruits, and instrumentalities of violations of the following statutes, as described more fully in Attachment B: 18 U.S.C. §§ 371 (Conspiracy); 1028 (Fraud in Connection with Identification Documents); 1028A (Aggravated Identity Theft); 1029 (Access Device Fraud); 1341 (Mail Fraud); 1343 (Wire Fraud); 1344 (Bank Fraud); and 1543 (False Use of a Passport (the "SUBJECT OFFENSES").

5. The facts set forth in this affidavit are based upon my personal observations, my training and experience, and information obtained from various law enforcement personnel and witnesses. This affidavit is intended to show merely that there

is sufficient probable cause for the requested complaints and warrants and does not purport to set forth all of my knowledge of or investigation into this matter. Unless specifically indicated otherwise, all conversations and statements described in this affidavit are related in substance and in part only, all amounts or sums are approximate, and all dates and times are on or about those indicated.

III. PREMISES/PROPERTY/PERSONS TO BE SEARCHED

6. The premises to be searched is the residence located at 86 Island Coral, Irvine, CA 92620 (the "JIA RESIDENCE") described in Attachment A-1. The property to be searched is the silver 2023 Porsche bearing temporary California license plate BX57G07 or California license plate 9EPD074, vehicle identification number WP0AB2A72PL130098 (the "WANG VEHICLE") described in Attachment A-2. The persons to be searched are KUNHUA JIA and XUE WANG described in Attachment A-3 and A-4. Attachments A-1, A-2, A-3, and A-4 are incorporated herein by reference.

IV. ITEMS TO BE SEIZED

7. The items to be seized are the evidence, fruits, and instrumentalities of violations of the SUBJECT OFFENSES, as described in Attachment B, which is incorporated herein by reference.

V. SUMMARY OF PROBABLE CAUSE

8. HSI, the Federal Deposit Insurance Corporation Office of the Inspector General ("FDIC-OIG"), and the Irvine Police Department ("Irvine PD"), have been investigating a large-scale

fraud ring that has been laundering millions of dollars from the proceeds of fraud schemes, including a scheme targeting elderly individuals across the United States.

9. In furtherance of the scheme targeting elderly individuals, JIA, WANG, and others known and unknown, rented residences in the Orange County area for short periods of time, usually one to three months, under fictitious identities by using counterfeit Chinese passports with fictitious names.

10. JIA, and others known and unknown, then opened bank accounts using counterfeit Chinese passports with fictitious identities and the addresses of the fraudulently rented residences to facilitate the scheme. In the course of the scheme, business accounts were also opened using fictitious businesses.

11. Victims of phone and e-mail scams, including many elderly individuals, were then instructed by the schemers to wire money into these accounts. After the funds were received, JIA and others would withdraw proceeds of the fraud, in the form of cash, at local bank branches.

VI. STATEMENT OF PROBABLE CAUSE

A. JIA USES A COUNTERFEIT PASSPORT TO WITHDRAW \$27,000 FRAUDULENTLY OBTAINED FROM VICTIM L.U.

12. In August 2022, I was contacted by Minnesota Bureau of Criminal Apprehension Special Agent Daniel Michener ("SA Michener") regarding 135 Mirth, Irvine, CA 92618 ("135 Mirth"), an address in Orange County, California, that was used in a scheme to defraud "L.U.", a resident in Minnesota.

13. From conversations with SA Michener and a review of his reports, as well as a Shakopee Police Department report, I learned the following:

a. On or about June 21, 2022, L.U. received a telephone call from an individual identifying himself as Benjamin S. Alpert, Deputy Inspector General with the United States Social Security Administration. This individual told L.U. that she needed to wire money to a secure account set up by the Social Security Administration to resolve a criminal matter that she was involved in. Per the caller's instructions, L.U. went to a Wells Fargo Bank branch on June 22, 2022 and wired \$27,500.00 to Chase Bank account number 856735078. The caller also provided the following information on the bank account:

i. Chase Bank, 5857 South Central Avenue, Unit 195, Los Angeles, CA 90001; Health Green Trading Inc., 1449 West Adams Blvd., Los Angeles, CA 90007, routing number 322271627.

b. The caller sent L.U. an image of what appeared to be a United States Social Security Administration PIV card with a picture of a white male and Benjamin S. Alpert's name. Through open-source checks, SA Michener concluded that the male in the picture was Benjamin M. Devlin, a Certified Public Accountant in Florida. SA Michener determined that Benjamin S. Alpert was a real Social Security Administration employee.

c. Chase Bank records for the account ending in 5078 obtained via a search warrant by Shakopee Police revealed the following:

i. The account was opened on May 31, 2022 in the name of Health Green Trading Company with an address of 135 Mirth; the sole signatory to the account was listed as "Hu Li," an officer of Health Green Trading Company.¹

ii. On June 22, 2022, the same date that L.U. wired \$27,500 to the Chase Bank account ending in 5078, an Asian male (later identified as JIA)² made four withdrawals, totaling \$27,500, at a Chase Bank branch in Tustin, California.

iii. A surveillance photograph provided by Chase Bank show JIA withdrawing \$500 from an ATM. JIA used a debit card associated with the account ending in 5078 to conduct this withdrawal.

iv. Surveillance photographs provided by Chase Bank show JIA conducting three cash withdrawals at the teller window in the amounts of \$15,000.00, \$6,000.00, and \$6,000.00. In one of the surveillance photographs, JIA can be seen using a passport to conduct the transaction.

d. Chase Bank filed two Cash Transaction Reports (CTRs) relating to these transactions. One CTR (No. 31000220344302) related to the \$15,000 cash withdrawal. The

¹ According to publicly available corporate records, Health Green Trading, Inc. was incorporated in California on May 31, 2022. Corporate records reflect that "LI HU" is the sole director, officer, and agent for the entity.

² I have reviewed the Chase bank surveillance photographs from the ATM and counter transactions discussed below and compared them to (1) the photograph on the Chinese passport used by JIA to enter the United States and (2) surveillance photographs of the individual believed to be JIA taken by Irvine PD Detective Voight at the JIA RESIDENCE, and determined that the photographs all depict the same person, JIA.

other CTR (No. 31000219722473) related to an attempted \$12,000 cash withdrawal.³ According to the CTRs, the individual conducting the cash withdrawals was "Hu Li" with a date of birth "2/7/84" and Chinese passport number E73911877.

e. Based on the information from Chase Bank and the CTRs, I believe that JIA used a counterfeit Chinese passport to withdraw the funds fraudulently obtained from L.U.

B. JIA AND WANG'S USE OF COUNTERFEIT PASSPORTS AND THE GOVERNMENT'S INTERCEPTION OF MAIL AND COUNTERFEIT PASSPORTS

14. In March 2023, I learned that Irvine Police Department had been investigating JIA, WANG, and others for criminal activity related to fraud. Irvine PD Detective Sarah Voigt first became aware of the activity sometime in October 2022 when calls from police departments across the country came in regarding Irvine addresses being used in the opening of bank accounts used by fraudsters to receive wire transfers from victims that were defrauded. Commonalities in these schemes included accounts being opened in Chinese names with Chinese passports. In the course of Irvine PD's investigation, 135 Mirth and several other Irvine addresses were identified and linked to fraudulent activity. Some of these properties were rented by JIA and WANG using fictitious names and counterfeit Chinese passports.

³ I believe that JIA did not conduct the \$12,000 cash withdrawal and instead conducted the two separate \$6,000 cash withdrawals in an effort to avoid bank reporting requirements.

1. Counterfeit Passports Used To Rent Irvine Properties

15. In or around January 2022, victim C.V., a resident of New Jersey, was defrauded after receiving a phone call from someone purporting to be an Internal Revenue Service agent. Per the caller's instructions, C.V. wire transferred \$55,650.00 from her Bank of America account to Wells Fargo account number #8567122414 in the name of Shuang Zhang ("Zhang"). Review of Wells Fargo account number #8567122414 showed that it was opened in Zhang's name on December 29, 2021, with a listed account address of 4790 Irvine Blvd., Ste. 105, Irvine, CA 92620 ("4790 Irvine Blvd."). The account also had a listed mailing address of 119 Charcoal, Irvine, CA 92620 ("119 Charcoal").

a. 4790 Irvine Blvd. is the address of a UPS Store. Two counterfeit Chinese passports with fictitious names were used to open this box. One passport was in the name of Shuang Zhang, and another was in the name of Bin Jia. The photo in Bin Jia's passport was that of JIA.

b. On March 21, 2023, I spoke with Det. Voigt who told me that the property manager of 119 Charcoal told her that JIA and his wife, WANG, were previous tenants of 119 Charcoal.

16. Irvine PD also determined from their investigation that several other properties had been rented by JIA and JIA's co-conspirators.

a. 159 Ingram, Irvine, CA 92620 ("159 Ingram"). Det. Voigt provided me copies of Chinese passports obtained from the property manager that were used by JIA and WANG to rent the

property. The passport under the name Ze, Wang, passport number ER2535563, had a picture of WANG. The passport under the name Fu Qi, passport number E92292568, had a picture of JIA. As described below, I conducted records checks for JIA and WANG and determined that they entered the United States using Chinese passports with different identification numbers and information. Accordingly, there is probable cause to believe that the Chinese passports used to rent the 159 Ingram property were counterfeit.

b. *109 Sideways, Irvine, CA 92618 ("109 Sideways") and 115 Desert Lotus, Irvine, CA 92618 ("115 Desert Lotus")*. Passport photographs of counterfeit Chinese passports used to rent these properties were in the names of Da Lu, passport number E92259568, and Lf LI, passport number E12893982. The passport under the name Da Lu had a picture of Sheng Song ("Song"), a co-conspirator.⁴ The passport under the name Lf LI had a picture of an unknown Asian female. Database checks of Chinese passports number E12893982 and E92259568 did not produce any positive results, therefore, I believe that these passports were counterfeit.

2. U.S. Mail Addressed to Irvine Addresses in the Names of Others Indicative of Fraudulent Activity

17. On March 8, 2023, Det. Voigt received a large box of mail from United States Postal Inspector Loren Rofe ("Inspector Rofe"). Inspector Rofe informed Det. Voight that the United

⁴ On March 21, 2023, Irvine PD Det. Voigt told me that in August 2022, Sheng told Irvine PD that he was being held against his will and forced to conduct work that he did not like for a male and a female.

States Postal Service ("USPS") held a large amount of mail they deemed fraudulent that was addressed to the following addresses:

- a. 186 Quiet Grove, Irvine, CA (94 items)
- b. 222 Harringay, Irvine, CA (501 items)
- c. 102 Menkar, Irvine, CA⁵ (45 items)
- d. 135 Mirth, Irvine, CA (118 items)
- e. 107 Sideways, Irvine, CA (71 items)
- f. 109 Sideways, Irvine, CA (183 items)
- g. 8364 Miramonte, Irvine, CA (20 items)
- h. 214 Radial, Irvine, CA (20 items)

18. The pieces of mail are largely from Bank of America and addressed to non-Asian names.

3. Interdiction of 10 Counterfeit Passports Addressed to Sheng Song at 159 Ingram

19. On or about March 16, 2023, I learned from HSI Task Force Officer and Diplomatic Security Service Special Agent Luis Orozco ("SA Orozco") that on March 2, 2023, United Parcel Service ("UPS") in Louisville, Kentucky intercepted 10 counterfeit Chinese passports destined for 159 Ingram, a property rented by JIA and WANG. The addressee was named Song Sheng and the counterfeit passports were addressed from a business in China. The passport photographs in each book depicted the same individual, but with slightly different photographs (e.g., changed facial expression or shirt color) and

⁵ On or about November 4, 2022, Irvine PD officers responded to a domestic violence call at 102 Menkar and encountered JIA and WANG. JIA was alleged to have beaten WANG.

different names. SA Orozco informed me that the names and biographical data were verified to be fraudulent.

4. Connection of JIA RESIDENCE to the Scheme and WANG's Use of a Counterfeit Passport

20. On March 17, 2023, Det. Voigt told me that JIA and WANG are currently residing at 86 Island Coral in Irvine (the JIA RESIDENCE). The property manager stated that JIA and WANG moved in on March 7, 2023. WANG used a Chinese passport under the name Ze Shu but with WANG's photograph on it to lease the property. I conducted a records check and determined that the Ze Shu passport was not used for any admission to or departure from the United States. Because the passport bears WANG's photograph, but a different name, and because there is no travel record relating to the Ze Shu passport, I believe that the Chinese passport used by WANG to lease the JIA RESIDENCE was counterfeit.

21. On March 17, 2023, at approximately 2:40 p.m., Irvine Detective Eric Han observed JIA at the residence.

5. Connection of WANG VEHICLE to the Scheme

22. According to records obtained by Det. Voight from Irvine Porsche, on January 12, 2023, WANG purchased a brand new 2023 Porsche Panamera for \$145,900 cash (the WANG VEHICLE). WANG used a Chinese driver's license and the same Chinese passport⁶ WANG used to book travel out of the United States to

⁶ According to Diplomatic Security Service Special Agent and HSI Task Force Officer Luis Orozco, WANG was issued an updated Chinese passport, passport number EG6180736, while she was in the United States. The exact issuance date cannot be determined at this time.

China on March 22, 2023, as discussed below. The WANG VEHICLE is registered to WANG at 159 Ingram. Irvine PD officers observed the WANG VEHICLE at 159 Ingram on February 24, 2023.

C. DEPARTMENT OF STATE AND UNITED STATES CUSTOMS AND BORDER PROTECTION RECORDS CHECKS

23. Records checks with the Department of State and United States Customs and Border Protection ("CBP") revealed the following information for JIA and WANG:

a. JIA

- i. Chinese passport number: EE8127705
- ii. Date of Birth: May 15, 1990
- iii. Visa Status: Visitor for Business and Pleasure (B1/B2)

b. WANG

- i. Chinese passport number: G39288428 (old); EG6180736 (current)
- ii. Date of Birth: October 2, 1989
- iii. Visa Status: Visitor for Business and Pleasure (B1/B2)

D. JIA AND WANG's PLANNED FLIGHTS

24. On March 21, 2023, Det. Voight informed me that Song was not responding to calls or messages Det. Voight made to follow up on Song's August 2022 report to Irvine PD, as noted in footnote 4 above. Suspecting that Song may have informed JIA or WANG of their contact with Irvine PD, I conducted travel record checks for JIA and WANG. Based on the results of those checks, I learned that WANG booked a one-way ticket to Xiamen, China,

departing Los Angeles International Airport on March 22, 2023. I also learned that JIA booked a one-way ticket to Dubai, United Arab Emirates, departing Los Angeles International Airport on March 23, 2023.

25. Given that JIA and WANG had only recently rented the JIA RESIDENCE, and WANG had recently purchased in cash the WANG VEHICLE, and given that Irvine PD had recently been in contact with Song, I believe that JIA and WANG were tipped-off to Irvine PD's investigation and are planning to flee the United States.

VII. TRAINING AND EXPERIENCE REGARDING THE SUBJECT OFFENSES

26. Based on my experience and training, and based on my consultation with other law enforcement officers, I know that:

a. It is common practice for individuals involved in bank fraud and passport fraud to use digital devices. Such digital devices are often used to facilitate, conduct, and track their fraudulent transactions. Suspects often use digital devices to perpetrate their crimes due to the relative anonymity gained by conducting financial transactions electronically or over the internet. They often employ digital devices for the purposes, among others, of: (1) applying online for fraudulent credit cards; (2) obtaining or storing personal identification information for the purpose of establishing or modifying fraudulent bank accounts and/or credit card accounts; (3) using fraudulently obtained bank accounts and/or credit card accounts to make purchases, sometimes of further personal information; (4) keeping records of their crimes; (5) researching personal information, such as social security numbers and dates of birth,

for potential identity theft victims. Such digital devices, as well as paper records of items described in this paragraph are commonly found in the houses, garages, and vehicles of those involved in fraud connected with identification documents and access device fraud.

b. It is also common for identity thieves to keep "profiles" of victims on digital devices. Such "profiles" contain the personal identifying information of victims, such as names, Social Security numbers, dates of birth, driver's license or state identification numbers, alien registration numbers, passport numbers, and employer or taxpayer identification numbers. Such profiles, as well as paper records of the same items described in this paragraph are commonly found in the houses, garages, and vehicles of those involved in identity theft and fraud.

c. It is also common for identity thieves to use digital devices to store information related to their identity theft crimes long after the crimes have been committed. This information can include logs of fraudulent transaction history; funds received; individuals and companies that have been victimized; payments from co-conspirators; and victim "profiles." Such records may also be kept in paper in the identity thieves' residences, garages, and vehicles.

d. It is common for identity thieves, and individuals engaged in bank fraud and identification document fraud to use equipment and software to print identification documents and cards, to create magnetic strips for documents and

cards, to use embossing machines to create documents and cards, to use laser printers to create documents and cards, and to use magnetic card readers to read and re-encode documents and cards. These items are commonly found in identity thieves' residences, garages, and vehicles. Software relevant to such schemes can often be found on digital devices, such as computers.

e. Individuals involved in fraud and counterfeit identity and various bank fraud schemes commonly keep proceeds of their schemes in their residences, garages, and vehicles.

f. I also know that it is common practice for members of these criminal groups to use safes and other secured containers as places to hold, maintain, hide, conceal, and store fraudulent cards and documents, and merchandise obtained with the same, as well as other materials relating to their criminal activities. By hiding the tools and fruits of fraud and identity theft in safes, criminals attempt to conceal the nature of their criminal activities to family, friends, and ultimately law enforcement. I also know that ultimately these criminal groups hope to obtain genuine currency but due to certain financial regulations, cash is difficult to deposit in traditional financial institutions without raising red flags. Accordingly, safes and secured containers are often used to hold the cash to prevent theft.

g. I know that individuals who participate in identity theft, bank fraud, and bank fraud schemes often have co-conspirators who they communicate with by phone, text message, social media and email, including by exchanging

photographs of stolen identity information and victims. In addition, such individuals often maintain contact information for their co-conspirators on their digital devices as well.

VIII. TRAINING AND EXPERIENCE ON DIGITAL DEVICES

27. As used herein, the term "digital device" includes any electronic system or device capable of storing or processing data in digital form, including central processing units; desktop, laptop, notebook, and tablet computers; personal digital assistants; wireless communication devices, such as telephone paging devices, beepers, mobile telephones, and smart phones; digital cameras; gaming consoles (including Sony PlayStations and Microsoft Xboxes); peripheral input/output devices, such as keyboards, printers, scanners, plotters, monitors, and drives intended for removable media; related communications devices, such as modems, routers, cables, and connections; storage media, such as hard disk drives, floppy disks, memory cards, optical disks, and magnetic tapes used to store digital data (excluding analog tapes such as VHS); and security devices. Based on my knowledge, training, and experience, as well as information related to me by agents and others involved in the forensic examination of digital devices, I know that data in digital form can be stored on a variety of digital devices and that during the search of a premises it is not always possible to search digital devices for digital data for a number of reasons, including the following:

28. Searching digital devices can be a highly technical process that requires specific expertise and specialized

equipment. There are so many types of digital devices and software programs in use today that it is impossible to bring to the search site all of the necessary technical manuals and specialized equipment necessary to conduct a thorough search. In addition, it may be necessary to consult with specially trained personnel who have specific expertise in the types of digital devices, operating systems, or software applications that are being searched.

29. Digital data is particularly vulnerable to inadvertent or intentional modification or destruction. Searching digital devices can require the use of precise, scientific procedures that are designed to maintain the integrity of digital data and to recover "hidden," erased, compressed, encrypted, or password-protected data. As a result, a controlled environment, such as a law enforcement laboratory or similar facility, is essential to conducting a complete and accurate analysis of data stored on digital devices.

30. The volume of data stored on many digital devices will typically be so large that it will be highly impractical to search for data during the physical search of the premises. A single megabyte of storage space is the equivalent of 500 double-spaced pages of text. A single gigabyte of storage space, or 1,000 megabytes, is the equivalent of 500,000 double-spaced pages of text. Storage devices capable of storing 500 or more gigabytes are now commonplace. Consequently, just one device might contain the equivalent of 250 million pages of data, which, if printed out, would completely fill three 35' x

35' x 10' rooms to the ceiling. Further, a 500 gigabyte drive could contain as many as approximately 450 full run movies or 450,000 songs.

31. Electronic files or remnants of such files can be recovered months or even years after they have been downloaded onto a hard drive, deleted, or viewed via the Internet.⁷ Electronic files saved to a hard drive can be stored for years with little or no cost. Even when such files have been deleted, they can be recovered months or years later using readily-available forensics tools. Normally, when a person deletes a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the hard drive until it is overwritten by new data. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space, i.e., space on a hard drive that is not allocated to an active file or that is unused after a file has been allocated to a set block of storage space, for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a swap or recovery file. Similarly, files that have been viewed on the Internet are often automatically downloaded into a temporary directory or cache. The browser typically maintains a fixed amount of hard drive space devoted to these files, and the files are only overwritten as they are replaced with more recently

⁷ These statements do not generally apply to data stored in volatile memory such as random-access memory, or "RAM," which data is, generally speaking, deleted once a device is turned off.

downloaded or viewed content. Thus, the ability to retrieve residue of an electronic file from a hard drive depends less on when the file was downloaded or viewed than on a particular user's operating system, storage capacity, and computer habits. Recovery of residue of electronic files from a hard drive requires specialized tools and a controlled laboratory environment. Recovery also can require substantial time.

32. Although some of the records called for by this warrant might be found in the form of user-generated documents (such as word processing, picture, and movie files), digital devices can contain other forms of electronic evidence as well. In particular, records of how a digital device has been used, what it has been used for, who has used it, and who has been responsible for creating or maintaining records, documents, programs, applications and materials contained on the digital devices are, as described further in the attachments, called for by this warrant. Those records will not always be found in digital data that is neatly segregable from the hard drive image as a whole. Digital data on the hard drive not currently associated with any file can provide evidence of a file that was once on the hard drive but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave digital data on the hard drive that show what tasks and processes on the computer were recently used. Web browsers, e-mail programs, and chat programs often store configuration data on the hard drive that can reveal

information such as online nicknames and passwords. Operating systems can record additional data, such as the attachment of peripherals, the attachment of USB flash storage devices, and the times the computer was in use. Computer file systems can record data about the dates files were created and the sequence in which they were created. This data can be evidence of a crime, indicate the identity of the user of the digital device, or point toward the existence of evidence in other locations. Recovery of this data requires specialized tools and a controlled laboratory environment, and also can require substantial time.

33. Further, evidence of how a digital device has been used, what it has been used for, and who has used it, may be the absence of particular data on a digital device. For example, to rebut a claim that the owner of a digital device was not responsible for a particular use because the device was being controlled remotely by malicious software, it may be necessary to show that malicious software that allows someone else to control the digital device remotely is not present on the digital device. Evidence of the absence of particular data on a digital device is not segregable from the digital device. Analysis of the digital device as a whole to demonstrate the absence of particular data requires specialized tools and a controlled laboratory environment, and can require substantial time.

34. Digital device users can attempt to conceal data within digital devices through a number of methods, including

the use of innocuous or misleading filenames and extensions. For example, files with the extension “.jpg” often are image files; however, a user can easily change the extension to “.txt” to conceal the image and make it appear that the file contains text. Digital device users can also attempt to conceal data by using encryption, which means that a password or device, such as a “dongle” or “keycard,” is necessary to decrypt the data into readable form. In addition, digital device users can conceal data within another seemingly unrelated and innocuous file in a process called “steganography.” For example, by using steganography a digital device user can conceal text in an image file that cannot be viewed when the image file is opened. Digital devices may also contain “booby traps” that destroy or alter data if certain procedures are not scrupulously followed. A substantial amount of time is necessary to extract and sort through data that is concealed, encrypted, or subject to booby traps, to determine whether it is evidence, contraband or instrumentalities of a crime. In addition, decryption of devices and data stored thereon is a constantly evolving field, and law enforcement agencies continuously develop or acquire new methods of decryption, even for devices or data that cannot currently be decrypted.

35. As discussed herein, based on my training and experience I believe that digital devices will be found during the search. I know from my training and experience and my review of publicly available materials that several hardware and software manufacturers offer their users the ability to unlock

their devices through biometric features in lieu of a numeric or alphanumeric passcode or password. These biometric features include fingerprint-recognition, face-recognition, iris-recognition, and retina-recognition. Some devices offer a combination of these biometric features and enable the users of such devices to select which features they would like to utilize.

36. If a device is equipped with a fingerprint scanner, a user may enable the ability to unlock the device through his or her fingerprints. For example, Apple Inc. ("Apple") offers a feature on some of its phones and laptops called "Touch ID," which allows a user to register up to five fingerprints that can unlock a device. Once a fingerprint is registered, a user can unlock the device by pressing the relevant finger to the device's Touch ID sensor, which on a cell phone is found in the round button (often referred to as the "home" button) located at the bottom center of the front of the phone, and on a laptop is located on the right side of the "Touch Bar" located directly above the keyboard. Fingerprint-recognition features are increasingly common on modern digital devices. For example, for Apple products, all iPhone 5S to iPhone 8 models, as well as iPads (5th generation or later), iPad Pro, iPad Air 2, and iPad mini 3 or later, and MacBook Pro laptops with the Touch Bar are all equipped with Touch ID. Motorola, HTC, LG, and Samsung, among other companies, also produce phones with fingerprint sensors to enable biometric unlock by fingerprint. The

fingerprint sensors for these companies have different names but operate similarly to Touch ID.

37. If a device is equipped with a facial-recognition feature, a user may enable the ability to unlock the device through his or her face. To activate the facial-recognition feature, a user must hold the device in front of his or her face. The device's camera analyzes and records data based on the user's facial characteristics. The device is then automatically unlocked if the camera detects a face with characteristics that match those of the registered face. No physical contact by the user with the digital device is necessary for the unlock, but eye contact with the camera is often essential to the proper functioning of these facial-recognition features; thus, a user must have his or her eyes open during the biometric scan (unless the user previously disabled this requirement). Several companies produce digital devices equipped with a facial-recognition-unlock feature, and all work in a similar manner with different degrees of sophistication, e.g., Samsung's Galaxy S8 (released Spring 2017) and Note8 (released Fall 2017), Apple's iPhone X (released Fall 2017). Apple calls its facial-recognition unlock feature "Face ID." The scan and unlock process for Face ID is almost instantaneous, occurring in approximately one second.

38. While not as prolific on digital devices as fingerprint- and facial-recognition features, both iris- and retina-scanning features exist for securing devices/data. The human iris, like a fingerprint, contains complex patterns that

are unique and stable. Iris-recognition technology uses mathematical pattern-recognition techniques to map the iris using infrared light. Similarly, retina scanning casts infrared light into a person's eye to map the unique variations of a person's retinal blood vessels. A user can register one or both eyes to be used to unlock a device with these features. To activate the feature, the user holds the device in front of his or her face while the device directs an infrared light toward the user's face and activates an infrared-sensitive camera to record data from the person's eyes. The device is then unlocked if the camera detects the registered eye. Both the Samsung Galaxy S8 and Note 8 (discussed above) have iris-recognition features. In addition, Microsoft has a product called "Windows Hello" that provides users with a suite of biometric features including fingerprint-, facial-, and iris-unlock features. Windows Hello has both a software and hardware component, and multiple companies manufacture compatible hardware, e.g., attachable infrared cameras or fingerprint sensors, to enable the Windows Hello features on older devices.

39. In my training and experience, users of electronic devices often enable the aforementioned biometric features because they are considered to be a more convenient way to unlock a device than entering a numeric or alphanumeric passcode or password. Moreover, in some instances, biometric features are considered to be a more secure way to protect a device's contents.

40. I also know from my training and experience, as well as from information found in publicly available materials including those published by device manufacturers, that biometric features will not unlock a device in some circumstances even if such features have been enabled. This can occur when a device has been restarted or inactive, or has not been unlocked for a certain period of time. For example, with Apple's biometric unlock features, these circumstances include when: (1) more than 48 hours has passed since the last time the device was unlocked; (2) the device has not been unlocked via Touch ID or Face ID in eight hours and the passcode or password has not been entered in the last six days; (3) the device has been turned off or restarted; (4) the device has received a remote lock command; (5) five unsuccessful attempts to unlock the device via Touch ID or Face ID are made; or (6) the user has activated "SOS" mode by rapidly clicking the right side button five times or pressing and holding both the side button and either volume button. Biometric features from other brands carry similar restrictions. Thus, in the event law enforcement personnel encounter a locked device equipped with biometric features, the opportunity to unlock the device through a biometric feature may exist for only a short time. I do not know the passcodes of any devices likely to be found during the search.

41. In my training and experience, the person who is in possession of a device or has the device among his or her

belongings at the time the device is found is likely a user of the device.

42. For these reasons, if while executing the warrant, law enforcement personnel encounter a digital device that may be unlocked using one of the aforementioned biometric features, the warrant I am applying for would permit law enforcement personnel to, with respect to any biometric sensor-enabled device that is (a) located at the JIA RESIDENCE or in the WANG VEHICLE and (b) falls within the scope of the warrant: (1) compel the use of JIA and/or WANG's thumb- and/or fingerprints on the device(s); and (2) hold the device(s) in front of the face of JIA and/or WANG with her/his eyes open to activate the facial-, iris-, and/or retina-recognition feature. With respect to fingerprint sensor-enabled devices, although I do not know which of the fingers are authorized to access any given device, I know based on my training and experience that it is common for people to use one of their thumbs or index fingers for fingerprint sensors; and, in any event, all that would result from successive failed attempts is the requirement to use the authorized passcode or password.

43. Other than what has been described herein, to my knowledge, the United States has not attempted to obtain this data by other means.

IX. CONCLUSION

44. For all the reasons described above, there is probable cause to believe that JIA committed False Use of a Passport, in violation of 18 U.S.C. § 1543.

45. Further, there is probable cause to believe that the items listed in Attachment B, which constitute evidence, fruits, and instrumentalities of violations of the Subject Offenses will be found in the JIA RESIDENCE, the WANG VEHICLE, and on the persons of JIA and WANG, as described in Attachments A-1 through A-4.

/s/

Daniel Ha, Special Agent
Homeland Security
Investigations

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by telephone on this 22nd day of March, 2023.

DOUGLAS F. McCORMICK

HONORABLE DOUGLAS F. MCCORMICK
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A-1

RESIDENCE TO BE SEARCHED

The premises to be searched is the residence located at 86 Island Coral, Irvine, CA 92620 (the "JIA Residence"). The JIA Residence is a northeast facing two story residential dwelling located at 86 Island Coral, Irvine CA 92620. The JIA Residence is the last property located along the third row of residences designated for even numbered addresses, "82 - 92". The number, "86" is embossed on the stucco located on the front side of the property underneath a lantern near the front door. A second lantern is located on the opposite side of the front door near the garage. The main body of the JIA Residence is painted beige. It has two north facing large windows located on the second floor with green shutters affixed to the outside stucco. The JIA Residence also has two car garage located next to front door walkway. The garage door appears to be painted light grey. The JIA Residence has tile roofing, light brown in color.

ATTACHMENT A-2

VEHICLE TO BE SEARCHED

The vehicle to be searched is a 2023 silver Porsche Panamera bearing temporary California license plate BX57G07 or California license plate 9EPD074, vehicle identification number WP0AB2A72PL130098 (the "WANG Vehicle"). The WANG Vehicle is registered to Xue WANG.

ATTACHMENT A-3

PERSON TO BE SEARCHED

The person of KUNHUA JIA, a 32-year-old Asian male (DOB 5/15/1990), approximately 5 feet, 10 inches tall and weighing approximately 180 pounds, and depicted in the photograph affixed to the Chinese passport number EE8127705, as shown below:



ATTACHMENT A-4

PERSON TO BE SEARCHED

The person of XUE WANG, a 33-year-old Asian female (DOB 10/2/1989), approximately 5 feet, 04 inches tall and weighing approximately 100 pounds, and depicted in the photograph affixed to the Chinese passport number G39288428, as shown below.



ATTACHMENT B

ITEMS TO BE SEIZED

1. The items to be seized are evidence, contraband, fruits, or instrumentalities of violations of 18 U.S.C. §§ 371 (Conspiracy); 1028 (Fraud in Connection with Identification Documents); 1028A (Aggravated Identity Theft); 1029 (Access Device Fraud); 1341 (Mail Fraud); 1343 (Wire Fraud); 1344 (Bank Fraud); and 1543 (False Use of a Passport (the "SUBJECT OFFENSES"), namely:

1. Records, documents, programs, applications, or materials relating to any passports, driver's licenses, and identification cards.

2. Records, documents, programs, applications, or materials relating to any bank accounts, credit card accounts, or other financial accounts;

3. Records, documents, programs, applications, or materials relating to identity information, including immigration, travel, or visa status, and other personal identifying information;

4. Records, documents, programs, applications, or materials relating to receipts or invoices for banking or financial activity not in the name of KUNHUA JIA or XUE WANG, but with the means of identification of another;

5. Records, documents, applications, or materials containing indicia of occupancy, residency, or ownership of any location being searched (including surveillance video);

6. Equipment and software used to print banking and identification cards, to create magnetic strips for banking and identification cards, to use embossing machines to create banking and identification cards, to use laser printers to create documents, and to use magnetic card readers to read and re-encode banking and identification cards;

7. U.S. currency in excess of \$10,000;

8. Gold and jewelry if worth is in excess of \$10,000;

9. Records, documents, programs, applications, or materials sufficient to show call log information, including all telephone numbers dialed from any of the digital devices and all telephone numbers accessed through any push-to-talk functions, as well as all received or missed incoming calls;

10. Records, documents, programs, applications, or materials sufficient to show SMS text, email communications, social media messages and accounts, or other text or written communications sent to or received from any of the digital devices and which relate to the SUBJECT OFFENSES;

11. Documents and keys relating to public storage units or safety deposit boxes; and

12. Any digital device used to facilitate the above-listed violations (and forensic copies thereof).

13. .

14. With respect to any digital device used to facilitate the SUBJECT OFFENSES:

i. evidence of who used, owned, or controlled the device at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, e-mail, e-mail contacts, chat and instant messaging logs, photographs, and correspondence;

ii. evidence of the presence or absence of software that would allow others to control the device, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

iii. evidence of the attachment of other devices;

iv. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the device;

v. evidence of the times the device was used;

vi. passwords, encryption keys, biometric keys, and other access devices that may be necessary to access the device;

vii. applications, utility programs, compilers, interpreters, or other software, as well as documentation and manuals, that may be necessary to access the device or to conduct a forensic examination of it;

viii. records of or information about Internet Protocol addresses used by the device;

ix. records of or information about the device's Internet activity, including firewall logs, caches, browser

history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.

2. As used herein, the terms "records," "documents," "programs," "applications," and "materials" include records, documents, programs, applications, and materials created, modified, or stored in any form, including in digital form on any digital device and any forensic copies thereof.

3. As used herein, the term "digital device" includes any electronic system or device capable of storing or processing data in digital form, including central processing units; desktop, laptop, notebook, and tablet computers; personal digital assistants; wireless communication devices, such as telephone paging devices, beepers, mobile telephones, and smart phones; digital cameras; gaming consoles (including Sony PlayStations and Microsoft Xboxes); peripheral input/output devices, such as keyboards, printers, scanners, plotters, monitors, and drives intended for removable media; related communications devices, such as modems, routers, cables, and connections; storage media, such as hard disk drives, floppy disks, memory cards, optical disks, and magnetic tapes used to store digital data (excluding analog tapes such as VHS); and security devices.

I. SEARCH PROCEDURE FOR DIGITAL DEVICES

4. In searching digital devices or forensic copies thereof, law enforcement personnel executing this search warrant will employ the following procedure:

a. Law enforcement personnel or other individuals assisting law enforcement personnel (the "search team") will, in their discretion, either search the digital device(s) on-site or seize and transport the device(s) to an appropriate law enforcement laboratory or similar facility to be searched at that location. The search team shall complete the search as soon as is practicable but not to exceed 120 days from the date of execution of the warrant. The government will not search the digital device(s) beyond this 120-day period without obtaining an extension of time order from the Court.

b. The search team will conduct the search only by using search protocols specifically chosen to identify only the specific items to be seized under this warrant.

i. The search team may subject all of the data contained in each digital device capable of containing any of the items to be seized to the search protocols to determine whether the device and any data thereon falls within the list of items to be seized. The search team may also search for and attempt to recover deleted, "hidden," or encrypted data to determine, pursuant to the search protocols, whether the data falls within the list of items to be seized.

ii. The search team may use tools to exclude normal operating system files and standard third-party software that do not need to be searched.

iii. The search team may use forensic examination and searching tools, such as "EnCase" and "FTK" (Forensic Tool

Kit), which tools may use hashing and other sophisticated techniques.

c. If the search team, while searching a digital device, encounters immediately apparent contraband or other evidence of a crime outside the scope of the items to be seized, the team shall immediately discontinue its search of that device pending further order of the Court and shall make and retain notes detailing how the contraband or other evidence of a crime was encountered, including how it was immediately apparent contraband or evidence of a crime.

d. If the search determines that a digital device does not contain any data falling within the list of items to be seized, the government will, as soon as is practicable, return the device and delete or destroy all forensic copies thereof.

e. If the search determines that a digital device does contain data falling within the list of items to be seized, the government may make and retain copies of such data, and may access such data at any time.

f. If the search determines that a digital device is (1) itself an item to be seized and/or (2) contains data falling within the list of other items to be seized, the government may retain the digital device and any forensic copies of the digital device, but may not access data falling outside the scope of the other items to be seized (after the time for searching the device has expired) absent further court order.

g. The government may also retain a digital device if the government, prior to the end of the search period,

obtains an order from the Court authorizing retention of the device (or while an application for such an order is pending), including in circumstances where the government has not been able to fully search a device because the device or files contained therein is/are encrypted.

h. After the completion of the search of the digital devices, the government shall not access digital data falling outside the scope of the items to be seized absent further order of the Court.

5. In order to search for data capable of being read or interpreted by a digital device, law enforcement personnel are authorized to seize the following items:

a. Any digital device capable of being used to commit, further, or store evidence of the offense(s) listed above;

b. Any equipment used to facilitate the transmission, creation, display, encoding, or storage of digital data;

c. Any magnetic, electronic, or optical storage device capable of storing digital data;

d. Any documentation, operating logs, or reference manuals regarding the operation of the digital device or software used in the digital device;

e. Any applications, utility programs, compilers, interpreters, or other software used to facilitate direct or indirect communication with the digital device;

f. Any physical keys, encryption devices, dongles, or similar physical items that are necessary to gain access to the digital device or data stored on the digital device; and

g. Any passwords, password files, biometric keys, test keys, encryption codes, or other information necessary to access the digital device or data stored on the digital device.

6. During the execution of this search warrant, if JIA and/or WANG is reasonably believed by law enforcement to be a user of a biometric sensor-enabled device that is located at the JIA RESIDENCE, or in the WANG VEHICLE and falls within the scope of the warrant, the law enforcement personnel are authorized to: (1) depress the thumb- and/or fingerprints of JIA and WANG onto the fingerprint sensor of the device (only when the device has such a sensor), and direct which specific finger(s) and/or thumb(s) shall be depressed; and (2) hold the device in front of the face of JIA and WANG with his or her eyes open to activate the facial-, iris-, or retina-recognition feature, in order to gain access to the contents of any such device. In depressing a person's thumb or finger onto a device and in holding a device in front of a person's face, law enforcement may not use excessive force, as defined in Graham v. Connor, 490 U.S. 386 (1989); specifically, law enforcement may use no more than objectively reasonable force in light of the facts and circumstances confronting them

7. The special procedures relating to digital devices found in this warrant govern only the search of digital devices pursuant to the authority conferred by this warrant and do not

apply to any search of digital devices pursuant to any other court order.